Maj Todd Roman, SM Project Officer
Mr. Andrew "Jake" Jacobs, Strategy Officer

2014 Defense Health Information Technology Symposium

Cloud Computing in the Defense Health Agency

DHA Vision

"A joint, integrated, premier system of health, supporting those who serve in the defense of our country."

Learning Objectives

- Understand the Fundamental Benefits of Cloud Computing
- Realize Challenges for Cloud Adoption
- Identify Compliance with DoD Requirements for Entering the Cloud
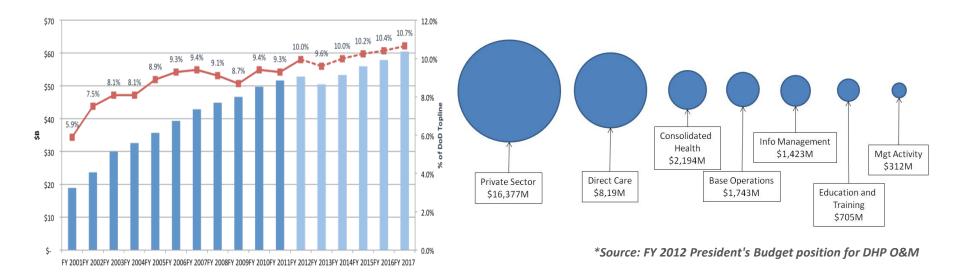- Recognize Contractual Concerns with DoD Cloud

Agenda

- Learning Objectives
- Benefits of Cloud Computing
  - ❑ Exchanging Data with Partners
- Challenges of Cloud Computing within Healthcare
  - ❑ DoD Cloud Computing Requirements
- Reaching the Cloud
  - ❑ Med-COI FOC State
- Contractual Concerns with DoD Cloud

Benefits of Cloud Computing

Cloud computing offers the government an opportunity to be more efficient, agile, and innovative through more effective use of IT investments.

Includes Normal Cost contributions to the Medicare Eligible Retiree Health Care Fund (MERHCF)

*Source: FY 2012 President's Budget position for DHP O&M

The government can use cloud computing to rid itself of billions annually in duplicative IT spending.

"Medically Ready Force…Ready Medical Force"

Exchanging Data with Partners

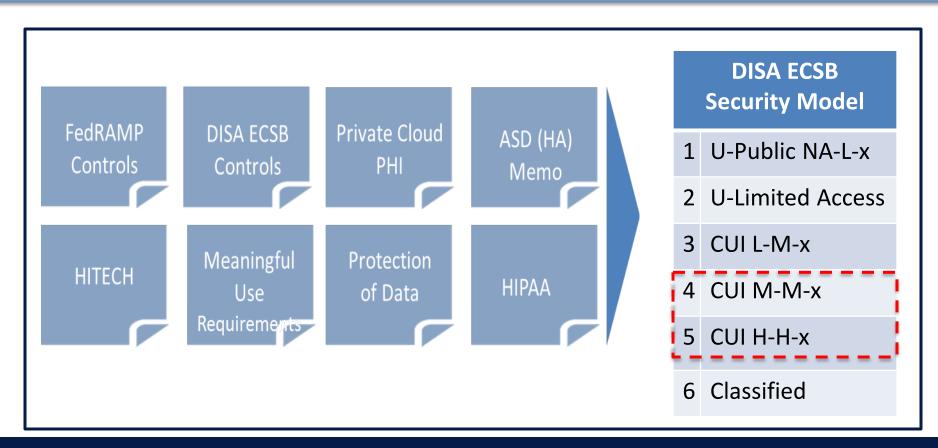|	
	Department of Veteran Affairs (VA)
	Department of Health and Human Services (HHS)
CMS CENTERS FOR MEDICARE & MEDICAID SERVICES	Centers for Medicare and Medicaid (CMS)
FDA	Federal Drug Administration (FDA)

HIE	Health Information Exchanges (HIE) (created by ACA)
	  -More than 100 across the country
	  -No Industry Standard Interfaces

The Office of the National Coordinator for Health Information Technology	Additional requirements to meet Office of National Coordinator (ONC) fo Health Information

Challenges of Cloud Computing within Healthcare

- Federal Cloud Computing Strategy

- Security Controls

- Compliance

- Cloud Brokerage

DoD Cloud Computing Requirements

FedRAMP Controls	DISA ECSB Controls	Private Cloud PHI	ASD (HA) Memo
HITECH	Meaningful Use Requirements	Protection of Data	HIPAA

DISA ECSB Security Model	
1	U-Public NA-L-x
2	U-Limited Access
3	CUI L-M-x
4	CUI M-M-x
5	CUI H-H-x
6	Classified

The DoD is currently operating between level 4 & 5 of the DISA ECSB Security model.

"Medically Ready Force…Ready Medical Force"

HITECH Act

Health Information Technology for Economic and Clinical Health (HITECH)

☑Data Ownership

☑Office of the General Council (OGC)

☑Privacy Office

While increasing the use of electronic health records, securing patient health Information (PHI) remains a major component of the HITECH.

Reaching the Cloud

Creating an enterprise-wide digital backbone

Increase Speed, Mobility and Collaboration of Healthcare

- ***Encourage*** the healthcare industry to meet DoD specific security requirements
- ***Separate*** the Healthcare Network from the DoD Information Network (DoDIN)
- ***Establish*** the Medical Community of Interest (MEDCOI)
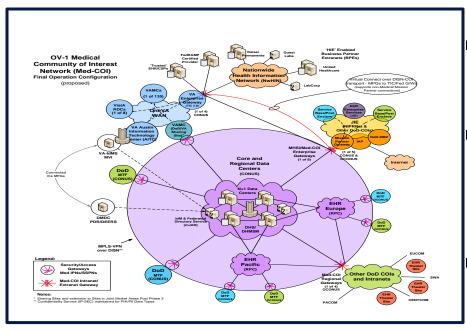- ***Support*** the Joint Information Environment (JIE)

Cloud Adoption

Catalyzing Cloud Adoption

- Leveraging cloud computing accelerators
- Ensuring a secure, trustworthy environment
- Streamlining procurement process
- Establishing cloud computing standards
- Recognizing the international dimensions of cloud computing
- Laying a solid governance foundation

*Source: http://csrc.nist.gov/groups/SNS/cloud-computing/, http://www.nist.gov/itl/cloud/index.cfm

Medical Community of Interest (Med-COI) FOC State

- DoD / VA Data Interoperability

- Commercial Business Partners and Service Providers

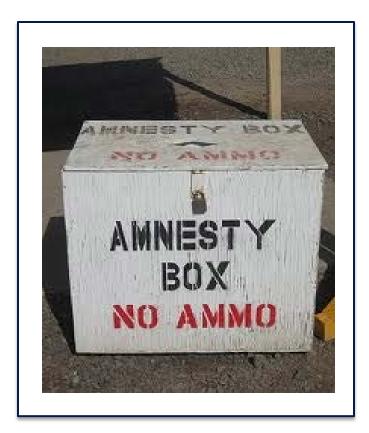- JIE Common / Core Services DoD Mission Partners

Contractual Concerns with DoD Cloud

- **Business Associates Agreements (BAAs)** - need to be evaluated down to the lowest subcontractor to support Privacy Impact Assessment (PIA)
- **Service Level Agreement (SLAs)** - need to be reviewed down to the lowest subcontractor level for PIA
- **Federal Risk and Authorization Management Program (FedRAMP) -** certifications need to be validated
- **Ongoing Monitoring** – What will you do to ensure monitoring according to FedRAMP/DoD requirements?
- **Private or Public Cloud considerations** – FedRAMP, NIST, and ECSB all require Private for PHI.
- **Cloud is NOT outsourced IT** – full Infrastructure, Platform and Software Security compliance needs to be assessed
- **Data Ownership** – Who owns the data within the system and what is it used for? What happens to the data when you terminate this contract? What happens if a subcontractor goes out of business?

Come see us if…

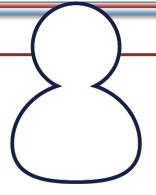- You're already operating in the cloud

- You plan to be in the cloud

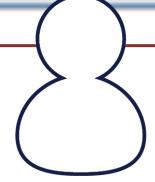# Please don't forget to submit your evaluations!

Speaker Info

Andrew "Jake" Jacobs
ITILv3, Net +, CHSP, CEP, VEP

Acting Branch Chief,
Strategy and Planning,
Innovation and Advanced Technology
Development (IATD) Division

Andrew.Jacobs@dha.mil
703-681-6759

MAJ Todd Roman, USAF
MSC, CAAMA

Project Officer, Secure Messaging

Defense Health Services Systems (DHSS)

Todd.Roman@dha.mil
703-681-9634

"Medically Ready Force...Ready Medical Force"